BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-129

4 APRIL 2001

HQ UNITED STATES AIR FORCE ACADEMY
Supplement 1

07 APRIL 2004

Communications and Information

TRANSMISSION OF INFORMATION VIA THE INTERNET

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ AFCIC/SCXX (Mr Paul Armel)
Certified by: HQ USAF/SCX (Col Stephen Quick)
Supersedes AFI 33-129, 1 August 1999.
Pages: 56
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 37-1, *Air Force Information Management* (will convert to AFPD 33-3); AFPD 35-2, *Public Communications Programs*; AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*; and AFPD 33-2, *Information Protection*. This instruction applies to all Air Force military and civilian personnel, including Air National Guard (ANG) and Air Force Reserve (AFRES), and their use of public internet and web technology such as web servers, web browsers, and file transfer protocol (FTP) software purchased and licensed by the United States Air Force (USAF), or privately licensed software used with proper approval on USAF-owned systems. This includes servers maintained by base communications personnel as well as servers maintained on small computers distributed throughout the Air Force. Failure to observe the prohibitions and mandatory provisions of this instruction as stated in paragraphs **6.1.1.** through **6.1.12.** by military personnel is a violation of Article 92, Uniform Code of Military Justice (UCMJ). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Direct questions or comments regarding the technical content of this instruction through appropriate major command (MAJCOM) channels to Headquarters Air Force Communications and Information Center (HQ AFCIC/SCXX), 1250 Air Force Pentagon, Washington DC 20330-1250. Refer recommended changes and conflicts between this and other publications, using AF Form 847, **Recommendation for Change of Publication**, through channels, to Headquarters Air Force Communications Agency (HQ AFCA/XPXP), 203 West Losey Street, Room 1060, Scott AFB IL 62225-5222. MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) send one copy of their supplement to HQ AFCA/XPXP. Refer to **Attachment 1** for a glossary of references and supporting information.

(USAFA) AFI 33-129, 4 April 2001, is supplemented as follows:

SUMMARY OF REVISIONS

This change incorporates interim change (IC) (see **Attachment 3**). This IC adds guidance on privacy policies, data collection on publicly accessible WEB sites, blocking Intranet/Extranet sites, pages or data, and Public Key Infrastructure. A (|) indicates revision from the previous edition.

1. Purpose. Use of the internet has dramatically increased in popularity as a means of obtaining and disseminating information worldwide. This instruction defines the roles and responsibilities of personnel using and maintaining internet access. It outlines responsibilities and procedures for accessing information and properly establishing, reviewing, posting, and maintaining government information on t he internet. It also covers the responsibilities and procedures for sending e-mail across the internet. Guidance on the technical network access is covered in AFI 33-115 Volume I (AFI 33-115V1), Network Management. Failure to observe the prohibitions and mandatory provisions of this instruction in paragraphs **6.1.1.** through **6.1.12.** by military personnel is a violation of Article 92, UCMJ. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal sanctions for violations of related laws.

2. Appropriate Use of the Internet . The internet provides opportunities for quick and efficient disseminating of information to the public, distributing information throughout the Air Force, and accessing information from a variety of sources. Information may be sent between offices or individuals, or be displayed on the web. The Air Force goal for the internet is to provide maximum availability at acceptable risk levels for Air Force members needing access for the execution of official business.

2. (USAFA) The 10th Communications Squadron (10 CS) will provide access to newsgroups that are essential to the official duties and education of United States Air Force Academy (USAFA) personnel. Organizational computer managers, in coordination with unit commanders or equivalent, must submit lists of required newsgroups to 10th Communications Squadron, Web Services (10 CS/SCBW) before the newsgroup will be made available. Subscriptions to listservers must be approved by unit commanders or equivalent and must be essential to the member's education and official duties.

3. Roles and Responsibilities :

3.1. Headquarters United States Air Force, Director of Communications and Information (HQ USAF/SC) will:

3.1.1. Develop policy and guidance governing use of the Internet.

3.1.2. Develop policy and guidance on operation, maintenance, and security of the systems that facilitate the use of the Internet.

3.1.3. Chair biennial policy review board to ensure policy is consistent with the needs of the Air Force.

3.2. Secretary of the Air Force, Office of Public Affairs (SAF/PA) will:

3.2.1. Develop policy and guidance governing the public communications program and the security and policy review program.

3.2.2. Develop policy and guidance for the integration of public Web sites into Air Force public communications plans and programs.

3.2.3. Serve as POC for developing a process for identifying appropriate information for posting to public Web sites.

3.2.4. Develop guidelines and standards for the appearance and content of public Web sites.

3.2.5. Establish and maintain a system to register Air Force Web sites that fulfill the Government Information Locator Service (GILS) requirements.

3.2.6. Serve as POC for routine reports submitted by the Joint Web Risk Assessment Cell which will be monitoring compliance with applicable Department of Defense and Air Force policies and procedures.

3.3. HQ USAF Functional Managers will:

3.3.1. Conduct annual multi-disciplinary reviews of subordinate public Web sites. Site reviews will look for information that is considered sensitive from the operational, public affairs, acquisition, technology, privacy, legal, and security perspectives. These reviews will coordinate across organizational boundaries as necessary (both vertically and horizontally) to ensure critical information is consistently controlled. Where ANG units are involved, coordination must include the respective State Adjutant General.

3.3.2. Determine the level of protection required when placing functional information on the Internet or when sending it by electronic mail (e-mail).

3.4. MAJCOMs/FOAs/DRUs will:

3.4.1. Establish localized plans and procedures for the establishment, maintenance, and review of their Web sites.

3.4.2. Develop effective operations security (OPSEC) programs to ensure critical information and OPSEC indicators are consistently controlled according to AFI 10-1101, *Operations Security*.

3.4.3. Establish and maintain official public access Web sites outside the firewall and other controlled access Web sites inside the firewall for internal uses. Register these sites with Air ForceLINK and verify registration annually.

3.4.4. Provide local index of subordinate Web sites by linking to Air ForceLINK.

3.4.5. Ensure all public Web sites are reviewed by PA prior to their launch. ANG units will coordinate with their Public Affairs Officer (PAO) prior to their launch. Establish record of review and approval for all subordinate sites.

3.4.6. Establish command-wide standards of appearance and function for public Web sites.

3.4.7. Conduct annual multi-disciplinary reviews of subordinate public Web sites.

3.5. Air Force Educational Institutions will comply with Department of Defense Directive (DoDD) 5230.9, *Clearance of DoD Information for Public Release*, April 9, 1996; and AFI 35-205, *Air Force Security and Policy Review Program* ensuring that students and faculty are afforded the necessary latitude to conduct open scholarly/scientific collaboration.

3.6. Commanders and Supervisors will:

3.6.1. Ensure assigned personnel use government equipment for official or authorized use only.

3.6.2. Authorize only legal and ethical use of the internet that is in the best interest of the Air Force.

3.6.3. Authorize personal use of e-mail only when that use complies with all the stipulations below.

3.6.3.1. Does not interfere with the performance of official duties.

3.6.3.2. Is of reasonable duration and frequency.

3.6.3.3. Serves a legitimate Air Force interest such as notifying family of travel changes while on temporary duty (TDY), communications from place of duty required during duty hours, or morale purposes if stationed for an extended period away from home.

3.6.3.4. Creates no additional expense to the Air Force.

3.6.4. Obtain all internet access through the supporting C4 systems officer (CSO).

3.7. CSO will:

3.7.1. Efficiently manage base internet facilities to ensure only authorized equipment and software necessary to perform official government business is procured and maintained.

3.7.2. Ensure internet connectivity is monitored and controlled by the base network control center (BNCC).

3.7.3. Advertise this instruction to users of the internet.

3.7.4. Exercise authority to block any locally managed Intranet/Extranet site/page or data on a page that is or has the potential of being a security risk or contains inappropriate material. Upon recognition of such information the CSO immediately notifies the web server administrator or page maintainer of the violation. Once notified, the owner of the page, site, or data must immediately correct or justify the apparent violation (in writing) or the page, site, or data will be blocked.

3.7.4.1. The block remains in place until the violation is corrected.

3.7.4.2. Multiple offenses by the same web page maintainer or web server administrator results in de-certification and removal of their rights or privileges to post or publish web pages. Rights or privileges will be reinstated when the web page maintainer is retrained and re-certified, or replaced.

3.8. BNCC will:

3.8.1. Control all internet connections, to include military controlled access paths and alternate internet access paths, such as Internet Service Providers (ISP).

3.8.2. Ensure all traffic destined for other military sites (within the ".mil" domain) is only routed through military controlled networks (that is, traffic destined for military sites will not be routed through an ISP and traffic from an ISP will not be routed through the receiving base network to other military networks).

3.8.3. Ensure "af.mil" network domains are not advertised through ISP connections. ***NOTE:*** Only the Air Force Network Support Center, Gunter AFB AL is authorized to establish connections to the "af.mil" network domain.

3.8.4. Ensure access to the internet is secured to acceptable risk levels as defined in paragraph **11.**.

3.8.5. Perform regular network scans for vulnerabilities. Verbally report all negative findings immediately to the CSO and the web server administrator of the page or web server in question, followed by a written report.

3.9. C4 Systems Security Officer (CSSO). Where dial-up access is absolutely necessary, will notify supporting BNCC of the intent to use dial-up subscription services and ensure computers used for such access do not have an active network routing capability and are protected by the most current available virus protection.

3.10. Users will:

3.10.1. Use government equipment and access the internet only for official business or authorized activities.

3.10.2. Determine the sensitivity and apply appropriate protection to all information transmitted using the internet.

3.10.3. Adhere to copyright restrictions.

3.10.4. Protect passwords and access codes.

3.10.5. Ensure that all official records created while using the internet are placed in the official record management system (see AFI 33-322, *Records Management Program*).

3.10.5. (USAFA) USAFAnet electronic systems are not authorized records management systems.

3.11. Information Provider. Provides material (for example, text, graphics, and so forth) to the page maintainer for posting on the web. The information provider is the point of contact (POC) of the material's subject matter and is responsible for:

3.11. (USAFA) The page maintainer for USAFAnet is 10 CS/SCBW. All Internet (but not Intranet) materials must also be provided to Headquarters USAFA Public Affairs Office (HQ USAFA/PA) for approval after being cleared by 10 CS/SCBW.

3.11.1. Ensuring material is reviewed by the appropriate office according to USAF policies, and identifying security and access controls required before it is posted on the internet.

3.11.2. Ensuring material is properly cleared and documented for release on the internet by the releasing authority (see AFI 35-205 for release procedures and authority).

3.11.3. Validating the accuracy of all material provided to the page maintainer.

3.11.4. Ensuring outdated or superseded information is identified and promptly removed from the system.

3.12. Assistant Secretary of the Air Force, Acquisition (SAF/AQ) will establish, in coordination with SAF/PA, policy and guidance governing the review and release of information made available on public Web sites in the conduct of electronic commerce (e.g. Request for Proposals, Commerce Business Daily Notices, etc.).

3.13. Wing-Level Equivalent Commanders will:

3.13.1. Establish and maintain one official public access Internet site and separate, additional controlled access Web sites for internal use per wing-equivalent unit. Register these sites with Air ForceLINK and verify registration annually.

3.13.2. Establish local clearance and approval procedures in accordance with AFI 35-205 for posting information to the Web. Review and approve in accordance with SAF/AQ guidance information made available on public Web sites for the conduct of electronic commerce.

3.13.3. Maintain an index and registration for any necessary subordinate pages. Maintain a separate index for public access and restricted Web sites.

3.13.4. Ensure all public Web sites are reviewed by the wing PA prior to their launch. ANG units will include coordination with the PA for their respective Adjutants General. Establish a record of review and approval for all subordinate sites.

3.13.5. Conduct annual multi-disciplinary reviews of subordinate public Web sites.

3.14. Multi-Disciplinary Review Boards will consist of representatives from Communications and Information, Public Affairs, Legal, Contracting, and Operations as well as any other representatives necessary to address questions concerning the sensitivity of information on a public Web site. The site reviews will review publicly accessible Web sites to ensure information that is sensitive from the operational, public affairs, acquisition, technology, privacy, legal, or security perspective does not appear on the public Web site.

4. Web Administration .

4.1. Web Server Administrator. The top-level home page for each web server will have a web server administrator identified by name, office symbol, phone number, and e-mail address. This individual is the POC for customers having problems with web documents on that server.

4.1.1. The web server administrator is responsible for:

4.1.1.1. Maintaining the server's top-level home page.

4.1.1.2. Operation of the server.

4.1.1.3. Security of the server.

4.1.1.4. Maintaining access and security control features.

4.1.1.5. Ensuring designated approving authority (DAA) approval is reaccomplished if any configuration changes are made to the system.

4.1.1.6. Registering site with Air ForceLINK.

4.1.1.7. Ensuring all links from pages under their control are appropriate and valid.

4.1.1.8. Establishing procedures for page maintainers to place information on the web server.

4.1.1.9. Granting and monitoring write-access privileges.

4.1.1.10. Maintaining and evaluating audit control logs.

4.1.1.11. Gathering and analyzing performance data on servers under their control.

4.1.1.12. Developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

4.1.1.13. Coordinating mirror or replication sites with other system administrators.

4.1.1.14. Implementing security and access controls requested by page maintainers.

4.2. Page Maintainer. Each subordinate page under the top-level home page will have a POC identified for information on that page. Page maintainers are members of the organization having overall responsibility for the page's subject matter. They develop and maintain the actual information file and are responsible for ensuring both the page content and presentation is consistent with Air Force policy. Page maintainers assist the web server administrator with implementing the appropriate access and security controls to protect the information resource.

4.2.1. Each page maintainer is responsible for:

4.2.1.1. Developing and maintaining subordinate-level pages.

4.2.1.2. Reviewing, documenting, and obtaining release authority on material before posting it to the page.

4.2.1.3. Validating all links from pages under their control.

4.2.1.4. Ensuring proper access and security controls are in place and operational.

4.2.1.5. Maintaining access lists.

4.2.1.6. Ensuring user identifications (ID) and passwords are in compliance with Air Force and local security policy, and are current.

4.2.1.7. Ensuring outdated or superseded information is removed from the system.

4.2.1.8. Incorporating a feedback mechanism for users' comments.

4.3. (Added-USAFA) 10th Communications Squadron, Network Security (10 CS/SCBNS) is charged with maintaining appropriate access of the Internet. This includes blocking unauthorized sites in accordance with this instruction. If a blocked site is for official business, the customer will notify the first supervisor in their chain of command who is a commissioned officer or a civilian with the grade of GS-11 or higher. If that supervisor is willing to endorse the request, the supervisor shall forward the request to **mailto:unblock@afncc@usafa** with the full URL in the message body. (For example, cadets who need access to a site for academic reasons should have their instructor send the message.)

5. Requirements Processing . Follow AFI 33-103, *Requirements Development and Processing*, when submitting requirements for internet access, the need to place information on a web server, view information on the WWW, develop information to place on a web page, or obtain e-mail capability. The CSO develops technical solutions based on the entire base C4 infrastructure and internet needs. CSOs will limit the number of servers to the minimum number needed to distribute the information. One server may serve many different users and organizations.

6. Access to the Internet .

6.1. Accessing the internet through a government computer or network uses a government resource. Government-provided hardware and software are for conducting official and authorized government business. This does not prohibit commanders from authorizing personnel to use government resources to further their professional and military knowledge if they determine it is in the best interest of the government and authorization is documented by letter, local operating instruction, or explicit policy. Using the internet for other than authorized purposes may result in adverse administrative or disciplinary action. The following activities involving the use of government-provided computer hardware or software listed in paragraphs**6.1.1.** through **6.1.12.** are specifically prohibited:

6.1. (USAFA) The following activities involving the use of government-provided hardware, software, or infrastructure listed in paragraphs **6.1.13. (Added)** through **6.1.17. (Added)** are specifically prohibited:

6.1.1. Any use of government-provided computer hardware or software for other than official and authorized government business.

6.1.2. Activities for personal or commercial financial gain. This includes, but is not limited to; chain letters; commercial solicitation; and sales of personal property, except on authorized bulletin boards established for such use.

6.1.3. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, "hate literature," such as racist literature, materials or symbols (for example, swastikas, neo-Nazi materials, and so forth), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

6.1.4. Storing or processing classified information on any system not approved for classified processing.

6.1.5. Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

6.1.6. Participating in "chat lines" or open forum discussion unless for official purposes and after approval by appropriate Public Affairs channels.

6.1.7. Using another person's account or identity without appropriate authorization or permission.

6.1.8. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

6.1.9. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission (such as for legitimate system testing or security research).

6.1.10. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

6.1.11. Permitting any unauthorized individual access to a government-owned or government-operated system.

6.1.12. Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.

6.1.13. (Added-USAFA) Accessing computer resources for which a customer is not authorized by their department or account status.

6.1.14. (Added-USAFA) Taking any actions to become anonymous or untraceable, except where an organization has specifically established an anonymous "drop-box" in support of mission requirements.

6.1.15. (Added-USAFA) Any actions which could monopolize, interfere with, or disrupt network customers, services, or equipment unless coordinated with and approved by 10th Communications Squadron network administrators.

6.1.16. (Added-USAFA) Using any network-based software that maintains a constant connection to the network (for example, network-based screensavers, music servers, and so forth) which is not directly related to duty. FedCast and RealAudio connections for away-football games are authorized exceptions to this rule.

6.1.17. (Added-USAFA) Taking part in any of the following actions: transmitting wildcard e-mail or chain mail on the Internet; mailbombing any customer or system on the Internet; creating or transmitting a virus, worm, or similar program on the Internet.

6.2. Each Air Force base and deployed force package network will have a single, logical point of internet access provided and defended by the BNCC.

6.3. Dial-Up Internet Services. Dial-up access to internet service providers, such as America On Line, CompuServe, or others, is prohibited for users with internet access through base and deployed networks, except when an organizational subscription is established for official business and the account is specifically authorized by the unit commander (see paragraphs **3.8.** and **5.** for requirements identification and processing procedures).

6.3. (USAFA) Transmission Control Protocol/ Internet Protocol (TCP/IP) access to Internet Service Provider (ISP) for reasons other than official business is authorized in accordance with AFI 33-129, *Transmission Of Information Via The Internet,* paragraph **3.6.**

6.4. Non-Mission Related Internet Services. As stated in paragraph **3.7.**, the BNCC is responsible for controlling all internet access. For security reasons, devices that provide public access to the internet for non-mission related activities (typically located in the library or morale, welfare, and recreation [MWR] facilities) shall not be connected to the base network with the privileges of "af.mil" registered users. Only mission related activities shall be registered "af.mil" users. The BNCC may establish common access for non-mission related users provided these users are not allowed unauthorized access to base, Air Force, or government resources.

6.5. (Added-USAFA) 10 CS/SCBNS is charged with the responsibility to monitor the network for violations of, and to enforce, this instruction. 10 CS/SCBNS reserves the right to immediately terminate network access in those cases where allowing an activity to continue will disrupt network or computing services either at USAFA or at another location if the source of the disruption is traced to USAFA. 10 CS/SCBNS is obligated to scan network drives on a regular basis to determine if any unauthorized files are being stored on USAFAnet. Violations of AFI 33-129 or this supplement may result in administrative or legal actions against the individual. Suspicious activity should be reported to 10 CS/SCBNS.

7. Clearing and Releasing Information Placed on the Web or Other Bulletin Boards.

7.1. Office of Primary Responsibility (OPR). The OPR is the creator and/or focal point for specific material posted on the organizational home page. The OPR is responsible and accountable for protecting its information resource and ensuring the requirements for release of information are satisfied. The OPR must also determine which functional areas need to review the material and identify any risks associated with the release of information. Information released to the internet may only be done by, or with the written consent of the OPR.

7.1. (USAFA) The office of primary responsibility for USAFAnet is 10 CS/SCBW. Information released to the Internet must also be approved by HQ USAFA/PA.

7.2. Public Access Web Sites. Public Web sites exist as part of the Air Force's public communications program and contribute to the overall image of the Air Force, increased public trust and support, airmen morale and readiness, and global influence and deterrence. "Public access information" refers to information approved for "unlimited" worldwide access and distribution on the Internet. Public access information has no access or security controls to limit access to the information. Because public Web sites have global distribution, you must clear the information in accordance with AFI 35-205 and DoDD 5230.9. Public Web sites will not contain any classification or markings. Only information

made available on public Web sites for the conduct of electronic commerce is exempt from coordination with local PAOs prior to its public release.

7.2.1. Procedures for Clearing Information for Public Access.

7.2.1.1. Since the intended audience for public access information is the general public, no access or security controls are necessary. However, servers must ensure public access cannot contaminate Air Force pages or gain access to other parts of the Air Force system. Use the same process taken to release information in paper form to review information prior to release on the WWW. **Table 1.** identifies some of the directives or instructions applicable to any review of information for public release. Do not regard **Table 1.** as the sole source for identifying reviewing authorities. You may find additional guidance on the releasability of information with the PA, foreign disclosure office, the scientific and technical information (STINFO) officer, the Security Classification Guide, and the Operations Security (OPSEC) Guide.

7.2.1.2. When reviewing information for public release, remember that the information should be of value to the general public. Do not place information that has value to only military or other government agencies on internet pages with unlimited access.

7.2.2. Approval to Establish a Public Web Site. Approval authority for establishing public Web sites should correspond to existing authority to make public release of information (normally the wing commander). Organizations seeking to establish a public Web site must justify a wide public audience and coordinate with local PA (and in the case of ANG units, the State PAO) and SC prior to receiving release authority (generally unit commander) approval. Only information intended for unlimited distribution is appropriate for public Web sites. The decision to establish a public Web site must weigh the value added by the site to the Air Force public image and public communications program against the maintenance costs and potential security risks.

7.3. Limited Access. Each OPR should recognize that "limited access information" refers to that information released on the internet with restrictions on file or data base access appropriate for the type of information involved. This information has added safeguards that limit the access to specific individuals or groups. The OPR must determine the appropriate security and access controls required to safeguard the information (see **Table 2.**).

7.3.1. Procedures for Clearing Information for Limited Access. The same channels taken to release information in paper form is used to screen information for limited access. Since the internet provides access across a number of interconnected networks, information without access controls on a server directly connected to the internet is potentially available to anyone on the internet. When information is cleared for limited access, access controls and/or encryption is necessary to protect the information. Remember, the intended audience will vary depending upon the information and its potential intelligence value. Also remember that unclassified information when combined with other available information, may become sensitive or even classified. This presents a significant threat to the information resource. Where appropriate, refer to the Security Classification Guide or contact the OPSEC office or base information protect office for assistance. When in doubt, take the extra time--check it out.

7.3.1.1. To place information on the internet, the OPR must stay aware of the types of security and access controls possible and the vulnerabilities of each. **Table 2.** outlines generic security and access controls for the internet with the recommended employment of each. Also, use **Table 2.** as a guide to determine the acceptable risk for releasing information. If the network is

a non-public network (that is, an internal local area network [LAN] or base-wide metropolitan area network [MAN]), the physical layout of the network may already provide a certain level of access control that should be taken into consideration when determining acceptable risk.

7.4. Information Not Appropriate for Public Release. Under no circumstances will the following types of information be placed on web sites that are available to the general public. OPRs placing this information on limited access sites are responsible for meeting all DoD and Air Force requirements for safeguarding information:

7.4.1. Classified information (see AFI 31-401, *Information Security Program Management*).

7.4.2. Privacy Act protected information (see AFI 37-132, *Air Force Privacy Act Program* [will convert to AFI 33-332]).

7.4.3. For Official Use Only (FOUO) information (see AFI 37-131, *Freedom of Information Act Program* [will convert to AFI 33-331]).

7.4.4. DoD contractor proprietary information (see AFI 61-204, *Disseminating Scientific and Technical Information*).

7.4.5. STINFO (see AFI 61-204).

7.4.6. Unclassified information requiring special handling (see AFI 33-113, *Managing Messaging and Data Processing Centers*).

7.4.7. Critical information as outlined in AFI 10-1101, *Operations Security*. Sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information.

7.4.8. Freedom of Information Action (FOIA) exempt information for which the agency declines to make a discretionary disclosure (see AFI 37-131).

7.5. Document the Process. Prior to release, OPRs will coordinate and document the process used to review information destined for internet release. Review processes may vary depending on the type and value of the information you are considering releasing (that is, releasability of standard publications is determined prior to publication; a blanket review and clearance for unclassified standard publications are sufficient). Maintain completed “Internet Release Packages” in the OPR's official files until the corresponding information is removed from the internet. Maintain these files according to the office file plan and Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule*, Table 37-18, Rule 17 (will convert to AFMAN 33-339). The OPR is accountable in the event of unauthorized disclosure of limited access information.

7.6. Republishing of Base Newspapers on the Web. Base newspapers are established according to DoD Instruction (DODI) 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997; and AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*. Though generally public domain, base newspapers exist as part of the Air Force’s internal information program. While the publishing of base newspapers constitutes public release of information, the distribution is limited. Publishing on an unlimited access Web site constitutes global release. Therefore, some information appropriate for base newspapers is not appropriate for public access Web sites. You may reproduce the content of base newspapers for the Web if that content meets the restrictions provided in DoD’s Interim Policy, *Web Site Administration Policies & Procedures*, November 25, 1998. These restrictions include prohibitions against

posting names, locations, and specific identifying information about family members of DoD employees and military personnel. You must review all stories against Part V of the DoD policy prior to posting to public Web sites.

8. Internet Pages . A "page" is a document, including the text of the document, its structure, any links to other documents, images, and other media provided to a web browser in response to a request. A "home page" is the screen or page designed by an organization as its front page.

8.1. Types of Pages:

8.1. (USAFA) Any Internet home page which will address cadets or cadet activities must be approved by the Commandant of Cadets in addition to the regular approval process. Any Internet home page which will address Preparatory School cadet candidates must be approved by the Preparatory School commander or designated representative.

8.1.1. Public Access Pages (Organizational). Public access pages are intended for viewing by the general public, and the information that goes on these pages should be of interest to the general public. Information that would not be of interest to the general public should not be on a public access page. Universal source locator addresses should follow the standard protocol used throughout the web. For instance, a site representing all of Dover Air Force Base to the public would most logically be located at **http://www.dover.af.mil**. Bases/MAJCOMs should have only one official home page for the base that serves as the virtual "visitor's center" for that base/MAJCOM. The base PA will coordinate on the content and layout of the base's home page. Register the Uniform Resource Locator (URL) or "address" for the base home page with Air ForceLINK the "official" installation home page (see paragraph **14.**). Use a separate server or partition to prevent access to restricted information by non-Air Force personnel.

8.1.1. (USAFA) Any organization desiring an Internet Home Page must receive approval from the USAFAnet Configuration Control Board (CCB) via 10 CS/SCBW. Once approved, 10 CS/SCBW will notify HQ USAFA/PA to address the next stage of the approval process.

8.1.2. Limited Access Pages (Organizational). Limited access pages are intended for viewing by a limited audience. The audience for this information varies with the type of information. Air Force organizations that intend to use internet and web technology for distribution of information within the Air Force should develop an intranet or limited access pages rather than use public access pages on the WWW. An intranet is a limited access network that uses web technology but is not directly connected to the public internet. Information approved for limited release must have added safeguards and security controls to limit access by other internet users. Restrict pages and bulletin boards to selected users by accepting connects from internet protocol (IP) addresses ending in ".mil" or ".gov" and/or by requiring a password. (See **Table 1.** and **Table 2.** for minimum access/security control required for information types.)

8.1.2.1. Errors Generated by Restricted Pages. Errors generated by public attempts to access restricted pages should redirect the public to the root public page and should not include language like "Access Denied" or "Forbidden." Make redirection from restricted sites as transparent as possible to the public.

8.1.3. Individual Pages. Develop individual pages only if a page is suitable for a specific duty position. For example, an individual page may be appropriate for an organizational commander or director but is not appropriate for a flight or branch chief. Personal pages are normally inappropri-

ate; the rare exception being for specifically approved functions such as educational purposes. Under no circumstance should the page extend beyond the official duties and position of the individual. Listing hobbies, favorite vacation sites, family photos, resumes, and preferred web sites is not appropriate.

8.2. Page Components.

8.2.1. External Links.

8.2.1.1. The ability to hyperlink to sources external to your organization is a fundamental part of the WWW and can add significant value to the functionality of publicly accessible Air Force Web sites. Air Force activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web pages. Guidelines should consider the informational needs of personnel and their families, mission-related needs, and public communications and community relations' objectives. Ensure guidelines are consistent with the following considerations:

8.2.1.1.1. Links to non-DoD Web resources should support the organization's mission. Review external links periodically to ensure their continued suitability. If the content of a linked external site becomes questionable or objectionable, remove the link.

8.2.1.1.2. In accordance with DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998, do not provide product endorsements or preferential treatment on publicly accessible official DoD Web sites.

8.2.1.1.3. You may not accept payment of any kind in exchange for a link placed on an organization's publicly accessible official DoD Web site.

8.2.1.1.4. In accordance with DoD 5500.7-R, publicly accessible DoD Web sites shall not require or encourage users to choose any specific browser software. Use text or hyperlinked text to direct visitors to software download sites. Graphics or logos depicting companies or products shall not appear on publicly accessible DoD Web sites.

8.2.1.1.5. Organizations considering the use of "frames" technology to connect to external sites should consult legal counsel concerning trademark and copyright issues before establishing such links. Where "frames" technologies are used, Web site owners will ensure "frames" are not continued when links external to the site are activated.

8.2.1.1.6. Organizations are encouraged to link to authorized activities in support of the organization's mission, such as the Army and Air Force Exchange Service, the Navy Exchange Service Command, and the Marine Corps Exchange. If these sites contain commercial advertisements or sponsorships, the appropriate disclaimer shall be given.

8.2.1.1.7. When external links to non-government Web sites are included, the MAJCOM commander, or its subordinate organization, is responsible for ensuring that a disclaimer is made that neither Air Force nor the organization endorses the product or organization at the destination, nor does the Air Force exercise any responsibility over the content at the destination. This includes credits given to contractors who produce Air Force Web sites.

8.2.1.1.8. Once the decision is made to include a link to one non-DoD site, the organization may have to link to all similar sites.

8.2.1.1.9. Refrain from having pointers on public access pages that reference information

that is outside the mission or functional area of the OPR. In most cases, home pages should refer or point only to parent commands and/or subordinate units. Installation home pages should provide pointers to base organizations as well as to the MAJCOM-level home page. Similarly, organizational home pages should have pointers up and down the chain of command.

8.2.1.1.10. Public Web sites should not link to sites that are restricted from the public. Under certain circumstances, it may be appropriate to establish a link to a log-on site (password interface or other control mechanism) provided details about the site's controlled content are not revealed.

8.2.1.2. Restrictions on pointers for limited access pages are not as stringent as those for public access pages. Pointers may point to a variety of military, government, educational, and organizational pages that provide information for use in the performance of official duties. Pointers may point to commercial organizations only if the information is necessary to the performance of official duties.

8.2.1.3. Display the following disclaimer when linking to external sites: "The appearance of hyperlinks does not constitute endorsement by the U.S. Air Force of this Web site or the information, products, or services contained therein. For other than authorized activities such as military exchanges and morale, welfare and recreation sites, the U.S. Air Force does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site." This disclaimer may appear on the page or pages listing external links or through an intermediate "exit notice" page generated by the server machine whenever a request is made for any site other than an official DoD Web site (usually the .mil domain).

8.2.2. Meta-Indexes, Indexes, or Lists of Other Air Force and DoD Pages. Indexes and lists will only reside on MAJCOM and at Air Force Link, the Air Force's service-level site. Local pages should refer to these centralized lists. Additions, deletions, and changes to the Air Force index are sent via e-mail to the address listed on Air ForceLINK. MAJCOMs will extract their portion of the list from the Air ForceLINK index. Indexes and lists are limited to those sites that provide relevant information to the intended audience.

8.2.3. Phone Numbers and Electronic Mail Addresses. Placing directories of all telephone and electronic mail addresses on public pages is prohibited. Providing such addresses invites mass mailings by commercial agencies and exposes organizations to attempts to overwhelm or "Spam" local networks with thousands of simultaneous and unwanted electronic mail messages. This does not prevent organizations from putting this information on intranet, or internal web sites, using limited domain or other restrictions. In addition, public pages are encouraged to "publish" general numbers of services such as the base locator, public affairs, and other commonly requested resources.

8.2.4. Advertising. Commercial advertising and product endorsement on Air Force Web sites are prohibited.

8.2.5. Use of Graphics and Artwork. Great care must be taken when adapting existing artwork for use on internet projects. For instance, most licenses for software designed to prepare documents or briefings do not permit the user to use the graphics for other purposes. In addition, most artwork is

either copyrighted or proprietary and will not be used unless permission is gained from the originator in writing. Consultation with local legal staffs is essential.

9. Single Source Information. Information should remain as closely controlled by the source as possible to ensure its currency and accuracy. Do not copy files from other sources on the internet and place them on a home page. Reference this information rather than repeat it. This does not prevent information providers from mirroring or replicating information for performance or security reasons. However, when this is done, the information provider of the replicating file server should contact the OPR of the information to get written permission to replicate the information and must establish procedures for updating the information. In addition, the page manager or Web server administrator must verify the releasability of the information.

10. Approval to Operate a Server on the Internet :

10.1. DAA Approval. According to DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988; Air Force Systems Security Instruction (AFSSI) 5024 Vol III, *The Designated Approving Authorities Guide*; and AFPD 33-2, all systems must receive accreditation and authorization to operate by the appropriate DAA prior to actual use. This applies to all servers directly connected to the internet. You must perform a network risk analysis along with a network security plan (see AFSSI 5024 Vol I, *Certification and Accreditation (C&A)* , for directions in preparing a network risk analysis). Determine the appropriate level of security from the risk analysis. DAA approval is reaccomplished anytime there is a significant change in sensitivity of information provided on the server (that is, server initially accredited for public access information that now contains limited access information). Failure to reaccredit will result in disconnection.

10.1. (USAFA) Customers will not install or use network servers or gateways that have not been approved by the USAFAnet CCB. This specifically includes providing a (Protocols such as: SLIP, PPP, HTTP, FTP, Telnet) or similar connection to unauthorized customers where facilities make this possible.

10.2. Auditing of User Activity. Configure systems so that the system administrator can audit both incoming and outgoing user activities. Auditing of incoming user activities helps identify possible security threats as well as provide OPRs feedback on the usefulness of their information. Auditing of outgoing user activity helps ensure government systems are not misused. Organizations can keep misuse of computer systems to a minimum by training and educating personnel on proper uses of the internet and monitoring their activity. (Monitoring of communications circuits alone will not prevent misuse.) Filter all internet requests through a “proxy server” in order to effectively monitor outgoing and incoming activities.

10.3. DoD PKI Server Certificate. In accordance with Assistant Secretary of Defense, Command, Control, Communications, and Intelligence Memorandum, subject: “Department of Defense (DoD) Public Key Infrastructure (PKI),” Management and Use, August 12, 2000; all private Air Force web servers must be issued a DoD X.509 PKI Server Certificate and have 128-bit Secure Sockets Layer (SSL) using this certificate enabled at all times.

11. System Security Considerations .

11.1. Internet Vulnerabilities. Because the internet is a public network, information placed on the internet without access controls is available to everyone. Using access controls effectively reduces the risk of accessing information on the internet.

11.1.1. Internet Controls. Restricting access to information is only part of the security equation. The internet is an inherently unsecured network. Information packets traveling across the internet jump from node to node to travel from origin to destination. At any point along the way, interception of the information can occur. To prevent unauthorized disclosure of information, security controls must be implemented. Any security controls implemented in the internet must meet Federal Information Processing Standard (FIPS) 140-1, *Security Requirements for Cryptographic Modules*. Therefore, to fully protect information resources, it takes a combination of access and security controls.

11.1.2. Internet Threats--Structured and Unstructured Attacks. Internet access growth, coupled with the increase of information stored, processed, or transmitted on Air Force computer systems increase the threat and vulnerability of Air Force information resources. Network attacks from the internet primarily come in two forms--structured and unstructured.

11.1.2.1. Structured attacks are sophisticated and organized, and are the most severe threat to our systems and our information resource. Structured attacks come from groups of individuals who have common goals. These groups target specific systems or groups of systems for industrial and military espionage, malicious intentions, financial gains, and, or military operational advantage.

11.1.2.2. Unstructured attacks are less organized but usually employ the same techniques as structured attacks. For example, the common computer “hacker” is an unstructured attacker. These attackers pick their targets at random, probing different domains in search of common system vulnerabilities to exploit. Individual attackers infiltrate systems out of curiosity to boast their success in the hacker community, enabling them to achieve a higher status. They may, however, have malicious intentions (for example, implanting logic bombs, Trojan horses, denial of service attacks, or altering data) just to cause grief to the system's legitimate users.

11.1.2.3. Countering the Threat. The Air Force has implemented a robust program to thwart most of these threats through a program called “Information Protection.” The Air Force Information Warfare Center (AFIWC) is the Air Force's leader in identifying the threats and confronting attacks to our automated information systems. AFIWC works closely with the MAJCOM/base/wing information protection office. The local information protection office provides expertise in educating systems administrators, information providers, and page OPRs on current threats, vulnerabilities, and protection techniques. The skill and knowledge levels of the systems administrator, in concert with the applied technical solutions or “patches” available, are the key determinants in keeping a system and its information secure. In a web environment, the information providers are also key because they identify the value of the information and the type of access controls and techniques necessary to protect information from unauthorized disclosure. Systems administrators, information providers, and page OPRs must maintain a close working relationship with the information protection office to remain aware of the ever changing threat to information and systems, and to report any unusual activity on a system. Listed below are some of the common techniques used to attack a system or its information:

11.1.2.3.1. IP Spoofing. Potential intruders attempt to gain access to a system or its information by creating packets with spoofed (faked) source IP addresses. This exploits applications that use authentication-based IP addresses and leads to unauthorized user access, and possibly "root access" (the ability to control an entire computer system, even to the exclusion of the system owner). A seasoned systems administrator can thwart these techniques with information and software from the information protection office.

11.1.2.3.2. Packet Sniffers. Information traverses the internet in packets through a series of computers. These computers (routers, bridges) reside at any given point on the internet, and are most likely outside of DoD control. These computers are also vulnerable to the same computer threats as DoD systems, and an intruder may compromise them by gaining root access. Once an intruder has gained access, they can activate a program (such as a Trojan horse) to collect information traversing the computer (for example, internet domain, account names, IDs, and passwords). Generally, good password administration and encryption techniques can thwart this threat.

11.1.2.3.3. Trojan Horse. These are hidden computer viruses or viruses in disguise. Trojan horses are often computer programs embedded in other programs or software. This is done by the intruder so the user is unaware of the Trojan horse's presence or existence. Trojan horse programs do something the programmer intended but that the user would not approve of if they knew about it. A virus is a particular case of a Trojan horse that is able to spread to other programs. Some Trojan horses hide in a system and capture information (for example, IDs and passwords of legitimate users) so the programmer can return to the system at a later time to damage, destroy, or steal data. In the case of an ID/password capture or compromise, an intruder gains the capability of entering the system as a legitimate user.

11.1.2.3.4. Network Monitoring Attacks. Systems at risk are systems that offer remote access through remote login, TELNET, and FTP. This threat involves a monitoring tool that uses a promiscuous mode of a specific network interface to capture host and user authentication information on all newly opened FTP, TELNET, and remote sessions. Intruders typically install Trojan horse programs to support subsequent access to the compromised system and to hide their network monitoring process. This technique threatens all user account and password information derived from FTP, TELNET, and remote sessions passing through the same network as the compromised system.

11.1.3. Downloading Files from the Internet. To protect against downloading viruses, users must virus-check all downloaded files. This applies to sound and video files as well as files attached to e-mail messages. If possible, download files to a floppy disk and virus-check them before placing them on the computer's hard drive. If files are compressed, perform a second check of the decompressed files. To prevent the possibility of rapidly spreading a virus, do not download files to a network or shared drive. The Air Force allows the use of public domain or shareware software only after it is certified by a software testing facility. Such as the AFIWC at Kelly AFB TX, the Software Technology Support Center at Hill AFB UT, or the Standard Systems Group at Maxwell AFB-Gunter Annex AL (see AFI 33-114, *Software Management*).

11.1.4. User IDs and Passwords. The use of passwords on Air Force systems is governed by AFMAN 33-223, *Identification and Authentication*.

11.1.5. IDs and Password Protection. The internet is an unsecured network where compromise of a user ID and password can occur during open transmission. Do not transmit user IDs and passwords without encryption. Secure sockets layer (SSL) protocol provides a transmission level of encryption between the client and server machines. In addition to encryption protections for passwords, use one time password systems to ensure password integrity.

11.1.6. Access and Security Controls on Information. **Table 2.** provides guidance on access and security controls, and the vulnerability of various combinations of each. Use **Table 2.** in conjunction with **Table 1.** to help determine an acceptable level of risk for information release. Do not regard these tables as the sole source for this information.

11.1.7. OPSEC. The internet access available to personnel at home and at work is an additional security factor. OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. Policies against communicating with unauthorized personnel also apply to internet communications. News groups (Network News Transfer Protocol [NNTP], Usenet News, Chats, etc.) give personnel the opportunity to converse electronically to a worldwide audience. Military and government employees should refrain from discussing work-related issues in such open forums. Such discussions could result in unauthorized disclosure of military information to foreign individuals, governments, or intelligence agencies or the disclosure of potential acquisition sensitive information. For example, news media monitoring the internet may construe an individual's “chat” as an official statement or news release.

Table 1. Security for Information Placed on the Internet/WWW.

TYPE OF INFORMATION	GOVERNING PUBLICATIONS	REVIEW PROCESS INCLUDES	MINIMUM ACCESS/ SECURITY CONTROL
Public Access	AFI 35-205 AFI 35-206, Media Relations	Public Affairs (PA)	Unlimited/Unencrypted
Limited Access (see NOTE 1)	AFI 35-205 AFI 35-206 Other Sources As Required	Public Affairs (PA)	.mil & .gov/Unencrypted
Marked For Official Use Only (FOUO) (see NOTE 2)	AFI 37-131, paragraph 26	FOIA Manager	Password and ID
Privacy Act	AFI 37-132	Privacy Act Officer	Password and ID
DoD Contractor Proprietary Information	AFI 61-204	Contracting and Contractor's Written Consent	Password and ID
Freedom of Information Act (FOIA)-Exempt Information	AFI 37-131	FOIA Manager	Password and ID
Unclassified Scientific and Technical Information (STINFO)	AFI 61-204		
Distribution Statement A	AFPD 61-2, *Management of Scientific and Technical Information*- AFI 61-204	STINFO Officer Public Affairs (PA)	Unlimited/Unencrypted
Distribution Statement B	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/ Encrypted
Distribution Statement C	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/ Encrypted
Distribution Statement D	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/ Encrypted
Distribution Statement E	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/ Encrypted
Distribution Statement F	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/ Encrypted

NOTES:
1. Certain types of information, though unclassified, may still have restrictions of foreign access. If this possibility exists, consult your local Foreign Disclosure Office for assistance. When the possibility of information becoming sensitive when aggregated with other non-sensitive information exists, the OPRs should consult the Security Classification Guide and, or operations security officer for assistance.
2. Must meet the criteria for exemptions 2 through 9 under AFI 37-131, paragraph 10.

Table 2. Vulnerability of Information Placed on the Internet/WWW.

If Access Control is:	and Security Control is:	the Vulnerability is:	and the Web Documents Should be those that are:
Unlimited	Unencrypted	EXTREMELY HIGH--open to everyone on the internet worldwide	Publicly accessible, including STINFO -marked Distribution A
Limited by Internet Domain (e.g., .mil, .gov) or IP Address	Unencrypted	HIGH--Can spoof access controls; affords the lowest level of access control; and no encryption	Non-Sensitive; normally publicly accessible; OPR prefers material remain outside of public view
Limited Access by User ID and Password	Unencrypted	MODERATE--Can spoof access controls; affords the highest level of access control; however, can compromise user IDs and passwords since encryption is not used.	Non-Sensitive; limited to small groups; OPR prefers protection of material with higher confidence of security
Limited Access by Domain or IP Address	Encrypted	LOW--Provides encryption and the lowest level of access control	Sensitive; OPR prefers material protected with high confidence of security
Limited Access by User ID and Password	Encrypted	EXTREMELY LOW--Encryption with the highest level of access control	Sensitive; Privacy Act, FOUO; DoD Contractor Proprietary, and STINFO with Distribution B-F

12. Page Layout and Maintenance . You must ensure Internet pages are professionally presented, current, accurate, factual, and related to the organizational mission. Use images appropriate to the content; do not use images indiscriminately. Do not display indicators to incomplete paths or use the phrase “under construction;” do not introduce information or services until they are ready. Announce new, or substantially changed information on the home page. Every Internet page will contain the following information as a minimum:

12.1. Page OPR name.

12.2. Organization, office symbol, commercial phone number, and Defense Switched Network (DSN) phone number.

12.3. E-mail address.

12.4. Any disclaimers or restrictions that apply to the contents of the page.

13. Warning Notices and Banners . Ensure warning notices and banners are present on each home page. Tailor public site banners to the audience and type of information presented. Limited access sites must use the exact banner wording found in paragraph **13.2.**.

13. (USAFA) Public postings to any listserver, newsgroup, or similar forums will contain the following disclaimer: ***"The views expressed are those of the author and do not necessarily reflect the official policy or position of the U.S. Air Force, Department of Defense, or U.S. government."***

13.1. Public Pages. Public pages will have a banner prominently displayed or announced on at least the first page of all major sections of each Web site. Providing a statement such as "Please read this privacy and security notice" linked to the actual notice is satisfactory. Organizations shall avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or "warning" signs. If the Web site collects any information on usage or other log files, notify visitors what information is collected, why it is collected, and how it is used. Agencies subject to DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988, must comply with its provisions. Guidance on required text of the privacy and security notice for public access pages follows:

13.1.1. Privacy and Security Notice.

13.1.1.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use:

Link from Index.html pages – "Please read this privacy and security notice."

( ) - indicates sections to be tailored at the installation level

[ ] - indicates hyperlinks

* - indicates information located at the hyperlink destination indicated

PRIVACY AND SECURITY NOTICE

1. (Web site name) is provided as a public service by the ([unit or installation]).

2. Information presented on (Web site name) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. [Information concerning visitors'],* use of this site is collected for analytical and statistical purposes, such as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Raw data logs will only be used to identify individual users and their usage habits for authorized law enforcement investigations or national security purposes. These logs are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines]

6. Unauthorized attempts to deny service, upload information, change information, or to attempt to access a non-public site from this service are strictly prohibited and may be punishable under Title 18 of the U.S. Code to include the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to us using the (Unit or Installation) [Comment Form]

* Link from above - “information is collected” to the following text:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

Example: Information Collected from (DefenseLINK) for Statistical Purposes.

Below is an example of the information collected based on a standard request for a World Wide Web document:

xxx.yyy.com -- [28/Jan/1997:00:00:01 -0500] "GET/DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704

Mozilla 3.0/www.altavista.digital.com

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (....com) the requester is coming from a commercial address. Depending on the requester’s method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] -- this is the date and time of the request.

“GET /DefenseLINK/news/nr012797.html HTTP/1.0” -- this is the location of the requested file on (DefenseLINK).

200 -- this is the status code - 200 is OK - the request was filled.

16704 -- this is the size of the requested file in bytes.

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages.

www.altavista.digital.com - this indicates the last site the person visited, which indicates how people find (DefenseLINK).

Requests for other types of documents use similar information. No other user-identifying information is collected.

13.2. Limited Pages. Each page of a Web site restricted from public access will clearly state its restriction. Use the following words: “This site is intended for the use of the Air Force [or more restrictive audience] only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner and your unit public affairs office.” The page must also display the following banner: “This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Inter-

net access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes." Preface limited access information covered by AFI 61-204 with the appropriate distribution statement.

13.3. Educational Research, Studies, and Analysis. Research, studies, and analysis done for educational purposes will post the same warning banner as the paper products, as follows. "The views expressed are those of the author and do not reflect the official policy or position of the U.S. Air Force, Department of Defense, or the U.S. Government."

13.4. (Added-USAFA) The firewall, all Unix hosts, and all routers shall display the following banner:

13.4. (Added-USAFA) The firewall, all Unix hosts, and all routers shall display the following banner:

Welcome to USAFAnet

United States Air Force Academy

This is an official Department of Defense (DoD) computer system for authorized use only. All data contained on DoD computer systems is owned by DoD and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized personnel. THERE IS NO RIGHT TO PRIVACY ON THIS SYSTEM. Authorized personnel may give any potential evidence of crime found on DoD computer systems to law enforcement officials. USE OF THIS SYSTEM BY ANY CUSTOMER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING AND DISSEMINATION BY AUTHORIZED PERSONNEL. Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information of greater sensitivity than this system is authorized. USAFAnet is not accredited to process classified information. Unauthorized use could result in criminal prosecution. If you do not consent to these conditions, do not log in!

14. Registration of Uniform Resource Locators . All Web sites residing on Air Force systems, contracted using Air Force resources, or Air Force sponsored must register with Air ForceLINK at URL "http://www.af.mil/sites." The purpose of registering is to develop the Government Information Locator Service (GILS). At a minimum, register all Web servers with Air ForceLINK and the MAJCOM Web server administrator for inclusion in the master index of Air Force and MAJCOM Web servers. Whenever there is a need to access a higher order list of servers, organizations will point to the applicable list rather than replicate the information.

14.1. Maintaining Registration with Air ForceLINK and Notice of URL Changes and Deletions. Web page administrators are required to ensure the currency of their registration with Air ForceLINK. Post changes to or deletions of public Web sites in advance. The change or deletion of public Web sites without prior notice detracts from the Air Force image unless the Web site must be changed or deleted due to security or operational needs.

15. Government Information Locator Service . The purpose of GILS is to provide a convenient, organized system for the public to access federal information resources. The Air Force point of entry into GILS is Air ForceLINK and its associated public access pages. All public access pages are required to develop an associated GILS Core Record. Office of Management and Budget (OMB) Bulletin 95-01, *Establishment of the Government Information Locator Service* describes GILS requirements; FIPS Publication 192, *Application Profile for the Government Information Locator Service (GILS)* describes mandatory and optional data elements required for the GILS Core Record. All Public Dissemination Products (PDP), must have an associated GILS Core Record posted to Air ForceLINK. PDPs are information products produced by the Air Force specifically for the public. You do not need to convert PDPs to an electronic media and place them on Air ForceLINK; however, the GILS Core Record must reflect where to gain access to the PDP.

16. Records Management . Do not use Internet pages or e-mail files to store official record copies of documents unless they contain an electronic records management application that manages the disposition of the records. Manage records according to AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323); AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338); and AFMAN 37-139 (will convert to AFMAN 33-339).

17. Electronic Mail . E-mail travels over the Non-secure Internet Protocol Router Network (NIPRNET) and other Internet lines. Sending an e-mail is not considered placing or releasing information on the Internet. E-mail is protected by passwords, direct addressing, and public law. Despite this protection, e-mail is vulnerable to interception. In addition, e-mail is recorded at the sending and receiving server. You must have access and security controls mentioned in paragraph **11.** in place to protect sensitive e-mail traffic. Determine the level of security measures required by the sensitivity of the information. Current e-mail packages do not guarantee delivery nor verify authenticity of the sender. To guarantee delivery, request a return receipt. To guarantee authenticity, verify information via telephone or additional e-mail. You can send non-critical unclassified sensitive information by using a password and user ID-protected e-mail. E-mail messages, including transmission data and attachments, may become official records, depending on the content of the message. Refer to records management publications listed in paragraph **16.** for guidance on managing e-mail as records.

18. Privacy Policies and Data Collection on Public WEB Sites . Unless specifically authorized as described below, Federal policy prohibits the use of web technology that collects user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors (i.e., “persistent cookies”) to DoD publicly accessible web sites. Persistent cookies (i.e., those that can be used to track users over time and across different web sites) are authorized only when there is a compelling need to gather the data on the site; appropriate technical procedures have been established to safeguard the data; the Secretary of Defense has personally approved using the cookie; and the web site gives clear and conspicuous notice of what information is collected or stored, why it is being done, and how it is to be used. DoD policy, however, does permit using other

"cookies" or web technology to collect or store information that does not identify the user, but only if users are advised of what information is collected or stored, why it is being done, and how it is to be used. This policy does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or intelligence agency of the Air Force.

JOHN S. FAIRFIELD, Lt General, USAF
DCS/Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDI 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publication*s, June 16, 1997

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoDD 5230.9, *Clearance of DoD Information for Public Release*, April 9, 1996

DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988

DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998

DoD *Interim Policy, Web Site Administration Policies & Procedures*, November 25, 1998

FIPS 140-1, *Security Requirements for Cryptographic Modules*

FIPS 192, *Application Profile for the Government Information Locator Service (GILS)*

OMB 95-01, *Establishment of the Government Information Locator Service*

Article 92, Uniform Code of Military Justice

Computer Fraud and Abuse Act of 1986

AFI 10-1101, *Operations Security*

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 31-401, *Information Security Program Management*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 33-103, *Requirements Development and Processing*

AFI 33-113, *Managing Messaging and Data Processing Centers*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

AFPD 33-2, *Information Protection*

AFMAN 33-223, I*dentification and Authentication*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 33-322, *Records Management Program*

AFMAN 33-323, *Management of Records*

AFPD 35-2, *Public Communications Programs*

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 35-206, *Media Relations*

AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*

AFPD 37-1, *Air Force Information Management* (will be converted to AFPD 33-3)

AFMAN 37-126, *Preparing Official Communications* (will convert to AFMAN 33-326)

AFI 37-131, *Freedom of Information Act Program* (will convert to AFI 33-331)

AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332)

AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFPD 61-2, *Management of Scientific and Technical Information*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFSSI 5004 Vol I, *The Certification and Accreditation (C&A) Process*

AFSSI 5024Vol III, *Designated Approving Authority Guide*

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRES—Air Force Reserve

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

AIS—Automated Information System

ANG—Air National Guard

BNCC—Base Network Control Center

CSO—C4 Systems Officer

CSSO—C4 Systems Security Officer

DAA—Designated Approving Authority

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DSN—Defense Switched Network

FIPS—Federal Information Processing Standards

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FTP—File Transfer Protocol

GILS—Government Information Locator Service

HTML—Hypertext Markup Language

HTTP—Hypertext Transfer Protocol

ID—Identification

IETF—Internet Engineering Task Force

IP—Internet Protocol

ISP—Internet Service Provider

LAN—Local Area Network

MAJCOM—Major Command

MAN—Metropolitan Area Network

MWR—Morale, Welfare, and Recreation

NIPRNET—Non-Secure Internet Protocol Router Network

NNTP—Network News Transfer Protocol

OMB—Office of Management and Budget

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PA—Public Affairs

PDP—Public Dissemination Products

PKI—Public Key Infastucture

POC—Point of Contact

RDT&E—Research Development, Test, and Evaluation

rlogin—Remote Login

SAF—Secretary of the Air Force

SMTP—Simple Mail Transfer Protocol

SSL—Secure Sockets Layer

STINFO—Scientific and Technical Information

TCP/IP—Transmission Control Protocol/Internet Protocol

TDY—Temporary Duty

UCMJ—Uniform Code of Military Justice

URL—Uniform Resource Locator

USAF—United States Air Force

WWW—World Wide Web

Terms

Air ForceLINK—The official Web information service for the Air Force.

Base Home Page—A public page that is the official base home page for an installation.

Client—A computer or program that requests a service of other computers or programs.

Cookies—Small bits of software placed on a web user's hard drive. Placeholders used to retain context during an individual user session.

C4 Systems Officer (CSO)—The term CSO identifies the supporting C4 systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base C4 systems responsibilities. At MAJCOM and other activities responsible for large quantities of C4 systems, it is the person designated by the commander as responsible for overall management of C4 systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

DefenseLINK—An official Web information service for the Department of Defense.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an automated information system (AIS) or network at an acceptable level of risk.

File Transfer Protocol (FTP)—A protocol for file transfer between computers; transferring files efficiently and reliably among computers and allowing the convenient use of remote file storage capabilities. A transfer protocol used to transfer files from one computer to another.

Firewall—A protection scheme that assists in securing internal systems from external systems.

Frames Technology—The capability to divide a web browser window into multiple window "panes" or display areas, each simultaneously displaying a different document, allowing multiple, independent document viewing within the same browser window.

Gopher—An information transfer protocol based on a menu interface. Gopher is a distributed document search and retrieval system; it combines the best features of browsing through collections of information and fully indexed databases. The protocol and software follow a client-server model, and permits users on a heterogeneous mix of desktop systems to browse, search, and retrieve documents residing on multiple distributed server machines.

Home Page—A starting point or center of an infostructure on the WWW. A typical home page will consist of hypertext links (pointers) to other web documents.

Hyperlink—A way to link access to information of various sources together within a Web document. A way to connect two Internet resources via a simple word or phase on which a user can click to start the connection.

Hypermedia—The extension of hypertext to things other than documents (for example, video and audio

clips).

Hypertext—A method for storing, retrieving, and presenting information based on the processing powerof computers. Allows computerized linking and almost instantaneous retrieval of information based on adynamic index.

Hypertext Markup Language (HTML)—The native language of the WWW. HTML is a subset of the more complex Standard Generalized Markup Language (SGML).

Hypertext Transfer Protocol (HTTP)—It is the primary protocol used to communicate on the WWW.

Information Protection Office—Formerly C4 Systems Security Office (CSSO).

Information Provider—The person or organization that provides information for posting on the Internet.

Infostructure—A group of Web documents linked together on one or more servers, usually providing information concerning a certain subject or idea.

Internet—An informal collection of government, military, commercial, and educational computer networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Internet Service Provider—A commercial entity providing data connectivity into the internet.

Intranet—A restricted-access network that works like the Web, but is not on it. Usually owned and managed by an organization, an Intranet enables an activity to share its resources with its employees without sensitive information being made available to everyone with Internet access. Intranets may allow connection outside of the Intranet to the Internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Internet Protocol (IP) Spoofing—The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to “change his identity” and appear as a valid machine within the network. This type of attack can be foiled by the filtering router which drops “outside” packets with an “inside” source address.

Limited Access—Limited access of Internet information applies to information that has been approved for limited access. This information has added safeguards that limit the access to a specific group or groups. According to AFI 35-205, the Office of Public Affairs (PA) will provide security and policy review for Internet information at the OPR’s request. The OPR must determine the appropriate security and access controls required to safeguard the information.

Limited Access by Domain—Limiting access by using the domain name (for example, .mil, .gov, .edu, and so forth) to restrict access of an area to a specific group or subgroup. Domains are established by the Internet Engineering Task Force (IETF) and assigned based on function or geography.

Limited Pages—Web pages intended for viewing by a limited audience.

Military Controlled Access Paths—Nonclassified networks or “links” that are leased, configured, managed, and secured by a government agency. This includes the unclassified but sensitive Internet Protocol Router Network (NIPRNET-AF, previously AFIN [Air Force Internet]) as well as dedicated links that have a node on the base network.

Network News Transfer Protocol (NNTP)—Also known as Usenet, specifies a protocol for the

distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the internet community. NNTP is designed so that news articles are stored in a central database, allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.

Page Maintainer—The creator and, or focal point for specific material posted on the organization's home page.

PKI Certificate—A digital representation of information that binds the user's identification with the user's public key in a trusted manner. At a minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Private Web Server—A web server that is designed for and/or provides information resources limited to a particular audience (i.e., DoD) or a subset thereof. (This includes web servers that provide interfaces to e-mail systems.) A private web server restricts, or attempts to restrict, general public access to it. The common means of restriction are domain restriction (e.g., .mil and/or .gov), filtering specific IP addresses, userid and/or password authentication, encryption (i.e., DoD certificates), and physical isolation. Any DoD operated web server that provides any information resources not intended for the general public shall be considered a private web server and subject to this policy.

Proxy Server—A server connected to the Internet through which all incoming and outgoing requests go through; used to enhance security and increase performance/efficiency.

Public Access—Public access of Internet information applies to information approved for unlimited public release. Public access information has no access or security controls to limit access to the information. This review determines degree of releasability only; actual release of the material is the decision of the originator (OPR).

Public Dissemination Products (PDP)—Information products produced by the Air Force specifically for the public.

Public Pages—Web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Scientific and Technical Information (STINFO)—STINFO includes all technical publications and documents generated by all Air Force-funded research development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports, that DoD could decide to disseminate to the public domain. It also encompasses engineering drawings, standards, specifications, technical manuals, blueprints, plans, instructions, computer software and documentation, photograph, technical orders, databases, and any other information that which is usable or adaptable design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment. It applies to recordings. It does not apply to cryptographic and communications security documents, communications and electronic intelligence, and other categories that the Director, National Security Agency, or the Chief, Central Intelligence Agency designates.

Secure Sockets Layer (SSL)—A security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Server—Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Simple Mail Transfer Protocol (SMTP)—The protocol used to send electronic mail on the Internet.

TELNET—Also known as rlogin, TELNET starts a remote session by specifying a computer to connect to. The command and program used to log in from one internet site to another. The TELNET command/ program gets you to the "login:" prompt of another computer or computer system. From that time until you finish the session, anything you type is sent to the other computer.

Transmission Control Protocol/Internet Protocol (TCP/IP)—The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Trojan Horse—A malicious program designed to break security or damage a system that is disguised as something else benign, such as a directory list, archive, a game, or a program to find and destroy viruses.

Uniform Resource Locators (URL)—An internet "address" of a resource. URLs can refer to Web servers, FTP sites, Gopher resources, News Groups, etc.

Web Browser—Software that acts as a client, allowing a person to retrieve information from various sources on the WWW.

Web Document—A physical or logical piece of information on the WWW.

Web Page—A single document that includes the text of the document, its structure, any links to other documents, images, and other media.

Web Server—A software/hardware combination that provides information resources to the WWW.

Web Server Administrator—The system administration for the Web server, usually referred to as the "Webmaster."

World Wide Web (WWW)—Uses the Internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the Internet by using hypertext and/or hypermedia documents.

Attachment 1 (USAFA)

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Terms

USAFAnet—The official government data communications network at the United States Air Force Academy. a

Cadet—A student at the United States Air Force Academy or a cadet candidate at the USAFA Preparatory School.

Attachment 2

IC 99-1 TO AFI 33-129, TRANSMISSION OF INFORMATION VIA THE INTERNET

1 AUGUST 1999

SUMMARY OF REVISIONS

This change incorporates IC 99-1. It updates and/or establishes HQ USAF/SC, SAF/PA, SAF/AQ, HQ USAF functional manager, MAJCOM/FOA/DRU, and wing-level equivalent commander roles and responsibilities. It establishes a requirement to create multi-disciplinary review boards and conduct annual Web site reviews. Change also expands guidance on managing Web sites, updates required warning notice and banner wording, and adds guidance for republishing base newspapers on the Web. A (|) indicates revision from the previous edition.

3.1. Headquarters United States Air Force, Director of Communications and Information (HQ USAF/SC) will:

3.1.1. Develop policy and guidance governing use of the Internet.

3.1.2. Develop policy and guidance on operation, maintenance, and security of the systems that facilitate the use of the Internet.

3.1.3. Chair biennial policy review board to ensure policy is consistent with the needs of the Air Force.

3.2.1. Develop policy and guidance governing the public communications program and the security and policy review program.

3.2.2. Develop policy and guidance for the integration of public Web sites into Air Force public communications plans and programs.

3.2.3. Serve as POC for developing a process for identifying appropriate information for posting to public Web sites.

3.2.4. Develop guidelines and standards for the appearance and content of public Web sites.

3.2.5. Establish and maintain a system to register Air Force Web sites that fulfill the Government Information Locator Service (GILS) requirements.

3.2.6. Serve as POC for routine reports submitted by the Joint Web Risk Assessment Cell which will be monitoring compliance with applicable Department of Defense and Air Force policies and procedures.

3.3. HQ USAF Functional Managers will:

3.3.1. Conduct annual multi-disciplinary reviews of subordinate public Web sites. Site reviews will look for information that is considered sensitive from the operational, public affairs, acquisition, technology, privacy, legal, and security perspectives. These reviews will coordinate across organizational boundaries as necessary (both vertically and horizontally) to ensure critical information is consistently controlled. Where ANG units are involved, coordination must include the respective State Adjutant General.

3.3.2. Determine the level of protection required when placing functional information on the Internet or when sending it by electronic mail (e-mail).

3.4.1. Establish localized plans and procedures for the establishment, maintenance, and review of their Web sites.

3.4.2. Develop effective operations security (OPSEC) programs to ensure critical information and OPSEC indicators are consistently controlled according to AFI 10-1101, *Operations Security*.

3.4.3. Establish and maintain official public access Web sites outside the firewall and other controlled access Web sites inside the firewall for internal uses. Register these sites with Air ForceLINK and verify registration annually.

3.4.4. Provide local index of subordinate Web sites by linking to Air ForceLINK.

3.4.5. Ensure all public Web sites are reviewed by PA prior to their launch. ANG units will coordinate with their Public Affairs Officer (PAO) prior to their launch. Establish record of review and approval for all subordinate sites.

3.4.6. Establish command-wide standards of appearance and function for public Web sites.

3.4.7. Conduct annual multi-disciplinary reviews of subordinate public Web sites.

3.12. Assistant Secretary of the Air Force, Acquisition (SAF/AQ) will establish, in coordination with SAF/PA, policy and guidance governing the review and release of information made available on public Web sites in the conduct of electronic commerce (e.g. Request for Proposals, Commerce Business Daily Notices, etc.).

3.13. Wing-Level Equivalent Commanders will:

3.13.1. Establish and maintain one official public access Internet site and separate, additional controlled access Web sites for internal use per wing-equivalent unit. Register these sites with Air ForceLINK and verify registration annually.

3.13.2. Establish local clearance and approval procedures in accordance with AFI 35-205 for posting information to the Web. Review and approve in accordance with SAF/AQ guidance information made available on public Web sites for the conduct of electronic commerce.

3.13.3. Maintain an index and registration for any necessary subordinate pages. Maintain a separate index for public access and restricted Web sites.

3.13.4. Ensure all public Web sites are reviewed by the wing PA prior to their launch. ANG units will include coordination with the PA for their respective Adjutants General. Establish a record of review and approval for all subordinate sites.

3.13.5. Conduct annual multi-disciplinary reviews of subordinate public Web sites.

3.14. Multi-Disciplinary Review Boards will consist of representatives from Communications and Information, Public Affairs, Legal, Contracting, and Operations as well as any other representatives necessary to address questions concerning the sensitivity of information on a public Web site. The site reviews will review publicly accessible Web sites to ensure information that is sensitive from the operational, public

affairs, acquisition, technology, privacy, legal, or security perspective does not appear on the public Web site.

7.2. Public Access Web Sites. Public Web sites exist as part of the Air Force's public communications program and contribute to the overall image of the Air Force, increased public trust and support, airmen morale and readiness, and global influence and deterrence. "Public access information" refers to information approved for "unlimited" worldwide access and distribution on the Internet. Public access information has no access or security controls to limit access to the information. Because public Web sites have global distribution, you must clear the information in accordance with AFI 35-205 and DoDD 5230.9. Public Web sites will not contain any classification or markings. Only information made available on public Web sites for the conduct of electronic commerce is exempt from coordination with local PAOs prior to its public release.

7.2.2. Approval to Establish a Public Web Site. Approval authority for establishing public Web sites should correspond to existing authority to make public release of information (normally the wing commander). Organizations seeking to establish a public Web site must justify a wide public audience and coordinate with local PA (and in the case of ANG units, the State PAO) and SC prior to receiving release authority (generally unit commander) approval. Only information intended for unlimited distribution is appropriate for public Web sites. The decision to establish a public Web site must weigh the value added by the site to the Air Force public image and public communications program against the maintenance costs and potential security risks.

7.6. Republishing of Base Newspapers on the Web. Base newspapers are established according to DoD Instruction (DODI) 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997; and AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*. Though generally public domain, base newspapers exist as part of the Air Force's internal information program. While the publishing of base newspapers constitutes public release of information, the distribution is limited. Publishing on an unlimited access Web site constitutes global release. Therefore, some information appropriate for base newspapers is not appropriate for public access Web sites. You may reproduce the content of base newspapers for the Web if that content meets the restrictions provided in DoD's Interim Policy, *Web Site Administration Policies & Procedures*, November 25, 1998. These restrictions include prohibitions against posting names, locations, and specific identifying information about family members of DoD employees and military personnel. You must review all stories against Part V of the DoD policy prior to posting to public Web sites.

8.1.2.1. Errors Generated by Restricted Pages. Errors generated by public attempts to access restricted pages should redirect the public to the root public page and should not include language like "Access Denied" or "Forbidden." Make redirection from restricted sites as transparent as possible to the public.

8.2.1. External Links.

8.2.1.1. The ability to hyperlink to sources external to your organization is a fundamental part of the WWW and can add significant value to the functionality of publicly accessible Air Force Web sites. Air Force activities will establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web pages. Guidelines should consider the informational needs of personnel and their families, mission-related needs, and public communications and community relations' objectives. Ensure guidelines are consistent with the following considerations:

8.2.1.1.1. Links to non-DoD Web resources should support the organization's mission. Review external links periodically to ensure their continued suitability. If the content of a linked external site becomes questionable or objectionable, remove the link.

8.2.1.1.2. In accordance with DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998, do not provide product endorsements or preferential treatment on publicly accessible official DoD Web sites.

8.2.1.1.3. You may not accept payment of any kind in exchange for a link placed on an organization's publicly accessible official DoD Web site.

8.2.1.1.4. In accordance with DoD 5500.7-R, publicly accessible DoD Web sites shall not require or encourage users to choose any specific browser software. Use text or hyperlinked text to direct visitors to software download sites. Graphics or logos depicting companies or products shall not appear on publicly accessible DoD Web sites.

8.2.1.1.5. Organizations considering the use of "frames" technology to connect to external sites should consult legal counsel concerning trademark and copyright issues before establishing such links. Where "frames" technologies are used, Web site owners will ensure "frames" are not continued when links external to the site are activated.

8.2.1.1.6. Organizations are encouraged to link to authorized activities in support of the organization's mission, such as the Army and Air Force Exchange Service, the Navy Exchange Service Command, and the Marine Corps Exchange. If these sites contain commercial advertisements or sponsorships, the appropriate disclaimer shall be given.

8.2.1.1.7. When external links to non-government Web sites are included, the MAJCOM commander, or its subordinate organization, is responsible for ensuring that a disclaimer is made that neither Air Force nor the organization endorses the product or organization at the destination, nor does the Air Force exercise any responsibility over the content at the destination. This includes credits given to contractors who produce Air Force Web sites.

8.2.1.1.8. Once the decision is made to include a link to one non-DoD site, the organization may have to link to all similar sites.

8.2.1.1.9. Refrain from having pointers on public access pages that reference information that is outside the mission or functional area of the OPR. In most cases, home pages should refer or point only to parent commands and/or subordinate units. Installation home pages should provide pointers to base organizations as well as to the MAJCOM-level home page. Similarly, organizational home pages should have pointers up and down the chain of command.

8.2.1.1.10. Public Web sites should not link to sites that are restricted from the public. Under certain circumstances, it may be appropriate to establish a link to a log-on site (password interface or other control mechanism) provided details about the site's controlled content are not revealed.

8.2.1.3. Display the following disclaimer when linking to external sites: “The appearance of hyperlinks does not constitute endorsement by the U.S. Air Force of this Web site or the information, products, or services contained therein. For other than authorized activities such as military exchanges and morale, welfare and recreation sites, the U.S. Air Force does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site.” This disclaimer may appear on the page or pages listing external links or through an intermediate “exit notice” page generated by the server machine whenever a request is made for any site other than an official DoD Web site (usually the .mil domain).

13. Warning Notices and Banners. Ensure warning notices and banners are present on each home page. Tailor public site banners to the audience and type of information presented. Limited access sites must use the exact banner wording found in paragraph **13.2.**.

13.1. Public Pages. Public pages will have a banner prominently displayed or announced on at least the first page of all major sections of each Web site. Providing a statement such as “Please read this privacy and security notice” linked to the actual notice is satisfactory. Organizations shall avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or “warning” signs. If the Web site collects any information on usage or other log files, notify visitors what information is collected, why it is collected, and how it is used. Agencies subject to DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988, must comply with its provisions. Guidance on required text of the privacy and security notice for public access pages follows:

13.1.1. Privacy and Security Notice.

13.1.1.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use:

Link from Index.html pages – “Please read this privacy and security notice.”

( ) - indicates sections to be tailored at the installation level

[ ] - indicates hyperlinks

* - indicates information located at the hyperlink destination indicated

PRIVACY AND SECURITY NOTICE

1. (Web site name) is provided as a public service by the ([unit or installation]).

2. Information presented on (Web site name) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. [Information concerning visitors’],* use of this site is collected for analytical and statistical purposes, such as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Raw data logs will only be used to identify individual users and their usage habits for authorized law enforcement investigations or national security purposes. These logs are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines]

6. Unauthorized attempts to deny service, upload information, change information, or to attempt to access a non-public sites from this service are strictly prohibited and may be punishable under Title 18 of the U.S. Code to include the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to us using the (Unit or Installation) [Comment Form]

* Link from above - "information is collected" to the following text:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

Example: Information Collected from (DefenseLINK) for Statistical Purposes

Below is an example of the information collected based on a standard request for a World Wide Web document:

xxx.yyy.com -- [28/Jan/1997:00:00:01 -0500] "GET/DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704

Mozilla 3.0/www.altavista.digital.com

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (....com) the requester is coming from a commercial address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] -- this is the date and time of the request.

"GET /DefenseLINK/news/nr012797.html HTTP/1.0" -- this is the location of the requested file on (DefenseLINK).

200 -- this is the status code - 200 is OK - the request was filled.

16704 -- this is the size of the requested file in bytes.

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages.

www.altavista.digital.com - this indicates the last site the person visited, which indicates how people find (DefenseLINK).

Requests for other types of documents use similar information. No other user-identifying information is collected.

13.2. Limited Pages. Each page of a Web site restricted from public access will clearly state its restriction. Use the following words: "This site is intended for the use of the Air Force [or more restrictive audience] only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner and your unit public affairs office." The page must also display the following banner: "This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes." Preface limited access information covered by AFI 61-204, *Disseminating Scientific and Technical Information*, with the appropriate distribution statement.

14.1. Maintaining Registration with Air ForceLINK and Notice of URL Changes and Deletions. Web page administrators are required to ensure the currency of their registration with Air ForceLINK. Post changes to or deletions of public Web sites in advance. The change or deletion of public Web sites without prior notice detracts from the Air Force image unless the Web site must be changed or deleted due to security or operational needs.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDI 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoDD 5230.9, *Clearance of DoD Information for Public Release*, April 9, 1996

DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988

DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998

DoD *Interim Policy, Web Site Administration Policies & Procedures*, November 25, 1998

FIPS 140-1, *Security Requirements for Cryptographic Modules*

FIPS 192, *Application Profile for the Government Information Locator Service (GILS)*

OMB 95-01, *Establishment of the Government Information Locator Service*

Article 92, Uniform Code of Military Justice

Computer Fraud and Abuse Act of 1986

AFI 10-1101, *Operations Security*

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 31-401, *Information Security Program Management*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 33-103, *Requirements Development and Processing*

AFI 33-113, *Managing Messaging and Data Processing Centers*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

AFPD 33-2, *Information Protection*

AFMAN 33-223, *Identification and Authentication*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 33-322, *Records Management Program*

AFMAN 33-323, *Management of Records*

AFPD 35-2, *Public Communications Programs*

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 35-206, *Media Relations*

AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*

AFPD 37-1, *Air Force Information Management* (will be converted to AFPD 33-3)

AFMAN 37-126, *Preparing Official Communications* (will convert to AFMAN 33-326)

AFI 37-131, *Freedom of Information Act Program* (will convert to AFI 33-331)

AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332)

AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFPD 61-2, *Management of Scientific and Technical Information*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFSSI 5004 Vol I, *The Certification and Accreditation (C&A) Process*

AFSSI 5024Vol III, *Designated Approving Authority Guide*

Abbreviations and Acronyms

AFCA--Air Force Communications Agency

AFI--Air Force Instruction

AFIWC--Air Force Information Warfare Center

AFMAN--Air Force Manual

AFPD--Air Force Policy Directive

AFRES--Air Force Reserve

AFSSI--Air Force Systems Security Instruction

AFSSM--Air Force Systems Security Memorandum

AIS--Automated Information System

ANG--Air National Guard

BNCC--Base Network Control Center

CSO--C4 Systems Officer

CSSO--C4 Systems Security Officer

DAA--Designated Approving Authority

DoD--Department of Defense

DoDD--Department of Defense Directive

DRU--Direct Reporting Unit

DSN--Defense Switched Network

FIPS--Federal Information Processing Standards

FOA--Field Operating Agency

FOIA--Freedom of Information Act

FOUO--For Official Use Only

FTP--File Transfer Protocol

GILS--Government Information Locator Service

HTML--Hypertext Markup Language

HTTP--Hypertext Transfer Protocol

ID--Identification

IETF--Internet Engineering Task Force

IP--Internet Protocol

ISP--Internet Service Provider

LAN--Local Area Network

MAJCOM--Major Command

MAN--Metropolitan Area Network

MWR--Morale, Welfare, and Recreation

NIPRNET--Non-Secure Internet Protocol Router Network

NNTP--Network News Transfer Protocol

OMB--Office of Management and Budget

OPR--Office of Primary Responsibility

OPSEC--Operations Security

PA--Public Affairs

PDP--Public Dissemination Products

POC--Point of Contact

RDT&E--Research Development, Test, and Evaluation

rlogin--Remote Login

SAF--Secretary of the Air Force

SMTP--Simple Mail Transfer Protocol

SSL--Secure Sockets Layer

STINFO--Scientific and Technical Information

TCP/IP--Transmission Control Protocol/Internet Protocol

TDY--Temporary Duty

UCMJ--Uniform Code of Military Justice

URL--Uniform Resource Locator

USAF--United States Air Force

WWW--World Wide Web

Terms

Air ForceLINK--The official Web information service for the Air Force.

Base Home Page--A public page that is the official base home page for an installation.

Client--A computer or program that requests a service of other computers or programs.

C4 Systems Officer (CSO)--The term CSO identifies the supporting C4 systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base C4 systems responsibilities. At MAJCOM and other activities responsible for large quantities of C4 systems, it is the person designated by the commander as responsible for overall management of C4 systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol “SC” which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

DefenseLINK--An official Web information service for the Department of Defense.

Designated Approving Authority (DAA)--Official with the authority to formally assume responsibility for operating an automated information system (AIS) or network at an acceptable level of risk.

File Transfer Protocol (FTP)--A protocol for file transfer between computers; transferring files efficiently and reliably among computers and allowing the convenient use of remote file storage capabilities. A transfer protocol used to transfer files from one computer to another.

Firewall--A protection scheme that assists in securing internal systems from external systems.

Frames Technology--The capability to divide a web browser window into multiple window "panes"or display areas, each simultaneously displaying a different document, allowing multiple, independent document viewing within the same browser window.

Gopher--An information transfer protocol based on a menu interface. Gopher is a distributed document search and retrieval system; it combines the best features of browsing through collections of information and fully indexed databases. The protocol and software follow a client-server model, and permits users on a heterogeneous mix of desktop systems to browse, search, and retrieve documents residing on multiple distributed server machines.

Home Page--A starting point or center of an infostructure on the WWW. A typical home page will consist of hypertext links (pointers) to other web documents.

Hyperlink--A way to link access to information of various sources together within a Web document. A way to connect two Internet resources via a simple word or phase on which a user can click to start the connection.

Hypermedia--The extension of hypertext to things other than documents (for example, video and audio clips).

Hypertext--A method for storing, retrieving, and presenting information based on the processing power of computers. Allows computerized linking and almost instantaneous retrieval of information based on a dynamic index.

Hypertext Markup Language (HTML)--The native language of the WWW. HTML is a subset of the more complex Standard Generalized Markup Language (SGML).

Hypertext Transfer Protocol (HTTP)--It is the primary protocol used to communicate on the WWW.

Information Protection Office--Formerly C4 Systems Security Office (CSSO).

Information Provider--The person or organization that provides information for posting on the Internet.

Infostructure--A group of Web documents linked together on one or more servers, usually providing information concerning a certain subject or idea.

Internet--An informal collection of government, military, commercial, and educational computer networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Internet Service Provider--A commercial entity providing data connectivity into the internet.

Intranet--A restricted-access network that works like the Web, but is not on it. Usually owned and managed by an organization, an Intranet enables an activity to share its resources with its employees without

sensitive information being made available to everyone with Internet access. Intranets may allow connection outside of the Intranet to the Internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Internet Protocol (IP) Spoofing--The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to “change his identity” and appear as a valid machine within the network. This type of attack can be foiled by the filtering router which drops “outside” packets with an “inside” source address.

Limited Access--imited access of Internet information applies to information that has been approved for limited access. This information has added safeguards that limit the access to a specific group or groups. According to AFI 35-205, the Office of Public Affairs (PA) will provide security and policy review for Internet information at the OPR's request. The OPR must determine the appropriate security and access controls required to safeguard the information.

Limited Access by Domain--Limiting access by using the domain name (for example, .mil, .gov, .edu, and so forth) to restrict access of an area to a specific group or subgroup. Domains are established by the Internet Engineering Task Force (IETF) and assigned based on function or geography.

Limited Pages--Web pages intended for viewing by a limited audience.

Military Controlled Access Paths--Nonclassified networks or “links” that are leased, configured, managed, and secured by a government agency. This includes the unclassified but sensitive Internet Protocol Router Network (NIPRNET-AF, previously AFIN [Air Force Internet]) as well as dedicated links that have a node on the base network.

Network News Transfer Protocol (NNTP)--Also known as Usenet, specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the internet community. NNTP is designed so that news articles are stored in a central database, allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.

Page Maintainer--The creator and, or focal point for specific material posted on the organization's home page.

Proxy Server--A server connected to the Internet through which all incoming and outgoing requests go through; used to enhance security and increase performance/efficiency.

Public Access--Public access of Internet information applies to information approved for unlimited public release. Public access information has no access or security controls to limit access to the information. This review determines degree of releasability only; actual release of the material is the decision of the originator (OPR).

Public Dissemination Products (PDP)--Information products produced by the Air Force specifically for the public.

Public Pages--Web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Scientific and Technical Information (STINFO)--STINFO includes all technical publications and documents generated by all Air Force-funded research development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports, that DoD could decide to

disseminate to the public domain. It also encompasses engineering drawings, standards, specifications, technical manuals, blueprints, plans, instructions, computer software and documentation, photograph, technical orders, databases, and any other information that which is usable or adaptable design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment. It applies to recordings. It does not apply to cryptographic and communications security documents, communications and electronic intelligence, and other categories that the Director, National Security Agency, or the Chief, Central Intelligence Agency designates.

Secure Sockets Layer (SSL)--A security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Server--Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Simple Mail Transfer Protocol (SMTP)--The protocol used to send electronic mail on the Internet.

TELNET--Also known as rlogin, TELNET starts a remote session by specifying a computer to connect to. The command and program used to log in from one internet site to another. The TELNET command/program gets you to the "login:" prompt of another computer or computer system. From that time until you finish the session, anything you type is sent to the other computer.

Transmission Control Protocol/Internet Protocol (TCP/IP)--The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Trojan Horse--A malicious program designed to break security or damage a system that is disguised as something else benign, such as a directory list, archive, a game, or a program to find and destroy viruses.

Uniform Resource Locators (URL)--An internet "address" of a resource. URLs can refer to Web servers, FTP sites, Gopher resources, News Groups, etc.

Web Browser--Software that acts as a client, allowing a person to retrieve information from various sources on the WWW.

Web Document--A physical or logical piece of information on the WWW.

Web Page--A single document that includes the text of the document, its structure, any links to other documents, images, and other media.

Web Server--A software/hardware combination that provides information resources to the WWW.

Web Server Administrator--The system administration for the Web server, usually referred to as the "Webmaster."

World Wide Web (WWW)--Uses the Internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the internet by using hypertext and/or hypermedia documents.

Attachment 3

INTERIM CHANGE (IC) 2001-1 TO AFI 33-129, TRANSMISSION OF INFORMATION VIA THE INTERNET

4 APRIL 2001

SUMMARY OF REVISIONS

This change incorporates interim change (IC) (see Attachment 3). This IC adds guidance on privacy policies, data collection on publicly accessible WEB sites, blocking Intranet/Extranet sites, pages or data, and Public Key Infrastructure. A (|) indicates revision from the previous edition.

3.7.4. Exercise authority to block any locally managed Intranet/Extranet site/page or data on a page that is or has the potential of being a security risk or contains inappropriate material. Upon recognition of such information the CSO immediately notifies the web server administrator or page maintainer of the violation. Once notified, the owner of the page, site, or data must immediately correct or justify the apparent violation (in writing) or the page, site, or data will be blocked.

3.7.4.1. The block remains in place until the violation is corrected.

3.7.4.2. Multiple offenses by the same web page maintainer or web server administrator results in de-certification and removal of their rights or privileges to post or publish web pages. Rights or privileges will be reinstated when the web page maintainer is retrained and re-certified, or replaced.

3.8.5. Perform regular network scans for vulnerabilities. Verbally report all negative findings immediately to the CSO and the web server administrator of the page or web server in question, followed by a written report.

6.1.2. Activities for personal or commercial financial gain. This includes, but is not limited to; chain letters; commercial solicitation; and sales of personal property, except on authorized bulletin boards established for such use.

10.3. DoD PKI Server Certificate. In accordance with Assistant Secretary of Defense, Command, Control, Communications, and Intelligence Memorandum, subject: “Department of Defense (DoD) Public Key Infrastructure (PKI),” Management and Use, August 12, 2000; all private Air Force web servers must be issued a DoD X.509 PKI Server Certificate and have 128-bit Secure Sockets Layer (SSL) using this certificate enabled at all times.

18. Privacy Policies and Data Collection on Public WEB Sites. Unless specifically authorized as described below, Federal policy prohibits the use of web technology that collects user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors (i.e., “persistent cookies”) to DoD publicly accessible web sites. Persistent cookies (i.e., those that can be used to track users over time and across different web sites) are authorized only when there is a compelling need to gather the data on the site; appropriate technical procedures have been established to safeguard the data; the Secretary of Defense has personally approved using the cookie; and the web site gives clear and conspicuous notice of what information is collected or stored, why it is being done, and how it is to be used. DoD policy, however, does permit using other “cookies” or web technology to collect or store information that does not identify the user, but only if users are advised of what information is collected or stored, why it is being done, and how it is to be used.

This policy does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or intelligence agency of the Air Force.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDI 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*, June 16, 1997

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

DoDD 5230.9, *Clearance of DoD Information for Public Release*, April 9, 1996

DoDD 5240.1, *DoD Intelligence Activities*, April 25, 1988

DoD 5500.7-R, *Joint Ethics Regulation* (JER), August 1993, with Change 4 dated August 6, 1998

DoD Interim Policy, *Web Site Administration Policies & Procedures*, November 25, 1998

FIPS 140-1, *Security Requirements for Cryptographic Modules*

FIPS 192, *Application Profile for the Government Information Locator Service (GILS)*

OMB 95-01, *Establishment of the Government Information Locator Service*

Article 92, Uniform Code of Military Justice

Computer Fraud and Abuse Act of 1986

AFI 10-1101, *Operations Security*

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 31-401, *Information Security Program Management*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 33-103, *Requirements Development and Processing*

AFI 33-113, *Managing Messaging and Data Processing Centers*

AFI 33-114, *Software Management*

AFI 33-115 Vol. 1, *Network Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

AFPD 33-2, *Information Protection*

AFMAN 33-223, *Identification and Authentication*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 33-322, *Records Management Program*

AFMAN 33-323, *Management of Records*

AFPD 35-2, *Public Communications Programs*

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 35-206, *Media Relations*

AFI 35-301, *Air Force Base Newspapers and Commercial Enterprise Publications Guidance and Procedures*

AFPD 37-1, *Air Force Information Management* (will be converted to AFPD 33-3)

AFMAN 37-126, *Preparing Official Communications* (will convert to AFMAN 33-326)

AFI 37-131, *Freedom of Information Act Program* (will convert to AFI 33-331)

AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332)

AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFPD 61-2, *Management of Scientific and Technical Information*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFSSI 5004 Vol I, *The Certification and Accreditation (C&A) Process*

AFSSI 5024Vol III, *Designated Approving Authority Guide*

Abbreviations and Acronyms

AFCA--Air Force Communications Agency

AFI--Air Force Instruction

AFIWC--Air Force Information Warfare Center

AFMAN--Air Force Manual

AFPD--Air Force Policy Directive

AFRES--Air Force Reserve

AFSSI--Air Force Systems Security Instruction

AFSSM--Air Force Systems Security Memorandum

AIS--Automated Information System

ANG--Air National Guard

BNCC--Base Network Control Center

CSO--C4 Systems Officer

CSSO--C4 Systems Security Officer

DAA--Designated Approving Authority

DoD--Department of Defense

DoDD--Department of Defense Directive

DRU--Direct Reporting Unit

DSN--Defense Switched Network

FIPS--Federal Information Processing Standards

FOA--Field Operating Agency

FOIA--Freedom of Information Act

FOUO--For Official Use Only

FTP--File Transfer Protocol

GILS--Government Information Locator Service

HTML--Hypertext Markup Language

HTTP--Hypertext Transfer Protocol

ID--Identification

IETF--Internet Engineering Task Force

IP--Internet Protocol

ISP--Internet Service Provider

LAN--Local Area Network

MAJCOM--Major Command

MAN--Metropolitan Area Network

MWR--Morale, Welfare, and Recreation

NIPRNET--Non-Secure Internet Protocol Router Network

NNTP--Network News Transfer Protocol

OMB--Office of Management and Budget

OPR--Office of Primary Responsibility

OPSEC--Operations Security

PA--Public Affairs

PDP--Public Dissemination Products

PKI--Public Key Infastucture

POC--Point of Contact

RDT&E--Research Development, Test, and Evaluation

rlogin--Remote Login

SAF--Secretary of the Air Force

SMTP--Simple Mail Transfer Protocol

SSL--Secure Sockets Layer

STINFO--Scientific and Technical Information

TCP/IP--Transmission Control Protocol/Internet Protocol

TDY--Temporary Duty

UCMJ--Uniform Code of Military Justice

URL--Uniform Resource Locator

USAF--United States Air Force

WWW--World Wide Web

Terms

Air ForceLINK--The official Web information service for the Air Force.

Base Home Page--A public page that is the official base home page for an installation.

Client--A computer or program that requests a service of other computers or programs.

Cookies--Small bits of software placed on a web user's hard drive. Placeholders used to retain context during an individual user session.

C4 Systems Officer (CSO)--The term CSO identifies the supporting C4 systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base C4 systems responsibilities. At MAJCOM and other activities responsible for large quantities of C4 systems, it is the person designated by the commander as responsible for overall management of C4 systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

DefenseLINK--An official Web information service for the Department of Defense.

Designated Approving Authority (DAA)--Official with the authority to formally assume responsibility for operating an automated information system (AIS) or network at an acceptable level of risk.

File Transfer Protocol (FTP)--A protocol for file transfer between computers; transferring files efficiently and reliably among computers and allowing the convenient use of remote file storage capabilities. A transfer protocol used to transfer files from one computer to another.

Firewall--A protection scheme that assists in securing internal systems from external systems.

Frames Technology--The capability to divide a web browser window into multiple window "panes" or display areas, each simultaneously displaying a different document, allowing multiple, independent document viewing within the same browser window.

Gopher--An information transfer protocol based on a menu interface. Gopher is a distributed document search and retrieval system; it combines the best features of browsing through collections of information and fully indexed databases. The protocol and software follow a client-server model, and permits users on a heterogeneous mix of desktop systems to browse, search, and retrieve documents residing on multiple distributed server machines.

Home Page--A starting point or center of an infostructure on the WWW. A typical home page will consist of hypertext links (pointers) to other web documents.

Hyperlink--A way to link access to information of various sources together within a Web document. A way to connect two Internet resources via a simple word or phase on which a user can click to start the connection.

Hypermedia--The extension of hypertext to things other than documents (for example, video and audio clips).

Hypertext--A method for storing, retrieving, and presenting information based on the processing power of computers. Allows computerized linking and almost instantaneous retrieval of information based on adynamic index.

Hypertext Markup Language (HTML)--The native language of the WWW. HTML is a subset of the more complex Standard Generalized Markup Language (SGML).

Hypertext Transfer Protocol (HTTP)--It is the primary protocol used to communicate on the WWW.

Information Protection Office--Formerly C4 Systems Security Office (CSSO).

Information Provider--The person or organization that provides information for posting on the Internet.

Infostructure--A group of Web documents linked together on one or more servers, usually providing information concerning a certain subject or idea.

Internet--An informal collection of government, military, commercial, and educational computer networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Internet Service Provider--A commercial entity providing data connectivity into the internet.

Intranet--A restricted-access network that works like the Web, but is not on it. Usually owned and managed by an organization, an Intranet enables an activity to share its resources with its employees without sensitive information being made available to everyone with Internet access. Intranets may allow connection outside of the Intranet to the Internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Internet Protocol (IP) Spoofing--The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to “change his identity” and appear as a valid machine within the network. This type of attack can be foiled by the filtering router which drops “outside” packets with an “inside” source address.

Limited Access--Limited access of Internet information applies to information that has been approved for limited access. This information has added safeguards that limit the access to a specific group or groups. According to AFI 35-205, the Office of Public Affairs (PA) will provide security and policy review for Internet information at the OPR’s request. The OPR must determine the appropriate security and access controls required to safeguard the information.

Limited Access by Domain--Limiting access by using the domain name (for example, .mil, .gov, .edu, and so forth) to restrict access of an area to a specific group or subgroup. Domains are established by the Internet Engineering Task Force (IETF) and assigned based on function or geography.

Limited Pages--Web pages intended for viewing by a limited audience.

Military Controlled Access Paths--Nonclassified networks or “links” that are leased, configured, managed, and secured by a government agency. This includes the unclassified but sensitive Internet Protocol Router Network (NIPRNET-AF, previously AFIN [Air Force Internet]) as well as dedicated links that have a node on the base network.

Network News Transfer Protocol (NNTP)--Also known as Usenet, specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the internet community. NNTP is designed so that news articles are stored in a central database, allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.

Page Maintainer--The creator and, or focal point for specific material posted on the organization's home page.

PKI Certificate--A digital representation of information that binds the user's identification with the user's public key in a trusted manner. At a minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Private Web Server--A web server that is designed for and/or provides information resources limited to a particular audience (i.e., DoD) or a subset thereof. (This includes web servers that provide interfaces to e-mail systems.) A private web server restricts, or attempts to restrict, general public access to it. The common means of restriction are domain restriction (e.g., .mil and/or .gov), filtering specific IP addresses, userid and/or password authentication, encryption (i.e., DoD certificates), and physical isolation. Any DoD operated web server that provides any information resources not intended for the general public shall be considered a private web server and subject to this policy.

Proxy Server--A server connected to the Internet through which all incoming and outgoing requests go through; used to enhance security and increase performance/efficiency.

Public Access--Public access of Internet information applies to information approved for unlimited public release. Public access information has no access or security controls to limit access to the information. This review determines degree of releasability only; actual release of the material is the decision of the originator (OPR).

Public Dissemination Products (PDP)--Information products produced by the Air Force specifically for the public.

Public Pages--Web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Scientific and Technical Information (STINFO)--STINFO includes all technical publications and documents generated by all Air Force-funded research development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports, that DoD could decide to disseminate to the public domain. It also encompasses engineering drawings, standards, specifications, technical manuals, blueprints, plans, instructions, computer software and documentation, photograph, technical orders, databases, and any other information that which is usable or adaptable design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment. It applies to recordings. It does not apply to cryptographic and communications security documents, communications and electronic intelligence, and other categories that the Director, National Security Agency, or the Chief, Central Intelligence Agency designates.

Secure Sockets Layer (SSL)--A security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Server--Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Simple Mail Transfer Protocol (SMTP)--The protocol used to send electronic mail on the Internet.

TELNET—Also known as rlogin, TELNET starts a remote session by specifying a computer to connect to. The command and program used to log in from one internet site to another. The TELNET command/ program gets you to the "login:" prompt of another computer or computer system. From that time until you finish the session, anything you type is sent to the other computer.

Transmission Control Protocol/Internet Protocol (TCP/IP)--The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Trojan Horse--A malicious program designed to break security or damage a system that is disguised as something else benign, such as a directory list, archive, a game, or a program to find and destroy viruses.

Uniform Resource Locators (URL)--An internet "address" of a resource. URLs can refer to Web servers, FTP sites, Gopher resources, News Groups, etc.

Web Browser--Software that acts as a client, allowing a person to retrieve information from various sources on the WWW.

Web Document--A physical or logical piece of information on the WWW.

Web Page--A single document that includes the text of the document, its structure, any links to other documents, images, and other media.

Web Server--A software/hardware combination that provides information resources to the WWW.

Web Server Administrator--The system administration for the Web server, usually referred to as the "Webmaster."

World Wide Web (WWW)--Uses the Internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the Internet by using hypertext and/or hypermedia documents.